

contained in a system of records from a source agency for use in a matching program.

(v) *Record.* Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(w) *Risk assessment.* An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity. Applies to manual and automated systems.

(x) *Routine use.* The disclosure of a record outside the Agency for a use that is compatible with the purpose for which the information was collected and maintained by the Agency. The routine use must be included in the published system notice for the system of records involved.

(y) *Source agency.* Any agency which discloses records contained in a system of records to be used in a matching program, or any state or local government, or agency thereof, which discloses records to be used in a matching program.

(z) *Statistical record.* A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(aa) *System of records.* A group of records under the control of the Agency from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all Privacy Act systems of records must be published in the FEDERAL REGISTER.

(bb) *Word processing equipment.* Any combination of electronic hardware and computer software integrated in a variety of forms (programmable software, hard wiring, or similar equip-

ment) that permits the processing of textual data.

(cc) *Word processing system.* A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written communications into a form suitable to the originator.

§317.4 Policy.

It is DCAA policy that personnel will comply with the DCAA Privacy Program and the Privacy Act of 1974. Strict adherence is necessary to ensure uniformity in the implementation of the DCAA Privacy Program and create conditions that will foster public trust. It is also agency policy to safeguard personal information contained in any system of records maintained by DCAA organizational elements and to make that information available to the individual to whom it pertains to the maximum extent practicable. DCAA policy specifically requires that DCAA organizational elements:

(a) Collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

(b) Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

(c) Inform individuals who are asked to supply personal information for inclusion in any system of records:

- (1) The authority for the solicitation.
- (2) Whether furnishing the information is mandatory or voluntary.
- (3) The intended uses of the information.

(4) The routine disclosures of the information that may be made outside of Department of Defense; and

(5) The effect on the individual of not providing all or any part of the requested information.

(d) Ensure that records used in making determinations about individuals and those containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained before making them available to any recipients

§317.5

outside of Department of Defense, other than a Federal agency, unless the disclosure is made under DCAA Regulation 5410.10, DCAA Freedom of Information Act Program (32 CFR part 290).

(e) Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertain or is pertinent to and within the scope of an authorized law enforcement activity.

(f) Notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such process is a matter of public record.

(g) Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

(h) Establish rules of conduct for DCAA personnel involved in the design, development, operation, or maintenance of any system of records and train them in these rules of conduct.

(i) Assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

(j) Permit individual access to the information pertaining to them maintained in any system of records, and to correct or amend that information, unless an exemption for the system has been properly established for an important public purpose.

(k) Provide, on request, an accounting of all disclosures of the information pertaining to them except when disclosures are made:

(1) To DoD personnel in the course of their official duties.

(2) Under 32 CFR part 290; and

(3) To another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.

(l) Advise individuals on their rights to appeal any refusal to grant access to or amend any record pertaining to them, and file a statement of disagree-

ment with the record in the event amendment is refused.

§317.5 Responsibilities.

(a) *Headquarters.* (1) The *Assistant Director, Resources* has overall responsibility for the DCAA Privacy Act Program and will serve as the sole appellate authority for appeals to decisions of respective initial denial authorities. Under his direction, the *Chief, Information Resources Management Branch*, under the supervision of the *Chief, Administrative Management Division* shall:

(i) Establish, issue, and update policies for the DCAA Privacy Act Program; monitor compliance with this part; and provide policy guidance for the DCAA Privacy Act Program.

(ii) Resolve conflicts that may arise regarding implementation of DCAA Privacy Act policy.

(iii) Designate an agency Privacy Act Advisor, as a single point of contact, to coordinate on matters concerning Privacy Act policy.

(iv) Make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in Privacy Act systems of records. This authority cannot be delegated.

(2) The *DCAA Privacy Act Advisor* under the supervision of the Chief, Information Resources Management Branch shall:

(i) Manage the DCAA Privacy Act Program in accordance with this part and applicable DCAA policies, as well as Department of Defense and Federal regulations.

(ii) Provide guidelines for managing, administering, and implementing the DCAA Privacy Act Program.

(iii) Implement and administer the Privacy Act program at the Headquarters.

(iv) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

32 CFR Ch. I (7-1-99 Edition)